REMARKS

The following remarks are prepared in response to the Office Action of February 24, 2005. Claims 1-10 remain pending in this application, after entry of this amendment. Reconsideration in light of the remarks made herein is respectfully requested.

Rejection of Claims 1-6 and 9-10 Under 35 U.S.C. § 102(b)

Claims 1-6 and 9-10 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Wasilewski et al.* (U.S. Patent No. 5,870,474, hereinafter *Wasilewski*). Applicant respectfully traverses.

Independent Claim 1

Independent claim 1 recites a data usage controlling apparatus that decrypts the encrypted condition information using the type 2 key and includes second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key. The data usage controlling apparatus prevents an unauthorized and unfair usage of the main data recorded in the recording medium, in a system for restricting the usage of the main data, by updating the condition information recorded in the recording medium in accordance with the usage of the main data. The condition information indicates, for example, how many times the main data has been used. The prevention of the unauthorized and unfair usage becomes possible by using the second updating means and the second encrypting means.

The unauthorized and unfair usage referred herein is such that the encrypted condition information and the encrypted type 2 key in the recording medium are copied to a different

recording medium (making unauthorized backup copies) before the main data is used, then the main data is used (a precondition is that, every time the main data is used, the system updates the condition information indicating the number of usage and such), and the unauthorized backup copies of the condition information and the type 2 key are restored to the recording medium after the main data is used (hereinafter referred to as "backup-restore attack"). The backup-restore attack is an unauthorized and unfair usage in a sense that it attempts to keep the condition information the same as before the usage even though the main data is actually used. The backup-restore attack is prevented by using the data usage controlling apparatus as recited in independent claim 1.

The type 1 key that is recorded in the storage unit different from the recording medium is updated by the second updating means, and the type 2 key which is used for encrypting the condition information in the recording medium is encrypted using the updated type 1 key. Then, the type 2 key in the recording medium is replaced with the newly encrypted type 2 key by the second encrypting means. Specifically, the type 1 key in a predetermined storage unit is updated according to the usage of the main data in a system in which (i) the encrypted type 2 key in the recording medium is decoded based on the type 1 key in a predetermined storage unit, (ii) the encrypted condition information is decoded using the decoded type 2 key, and (iii) thereby controlling the usage of the main data based on the obtained condition information. In such a system, it is not possible to make an unauthorized backup copy of the type 1 key in a different recording medium, and therefore the above described backup-restore attack does not work effectively.

Wasilewski discloses a technique of securely transmitting information. In data transmission between apparatuses, the control word (CW) is encrypted using the multi-session key (MSK) and stored in the entitlement control messages (ECM), and then transmitted. The MSK is encrypted by the public key encryption and then transmitted. The Examiner refers to Col. 9, lines 47-58 of *Wasilewski* as describing "decrypts the encrypted condition information using the type 2 key" as recited in independent claim 1. From this reference, it appears that the Examiner equates the type 2 key recited in independent claim 1 with the MSK of *Wasilewski*, and the condition information recited in independent claim 1 with the CW of *Wasilewski*.

However, the CW of *Wasilewski* is not updated in accordance with the usage of the main data. Rather, *Wasilewski* uses a random number that is updated every few seconds regardless of the usage of the main data in order for a secure transmission (See *Wasilewski*, Col. 8, lines 48-60). Thus, the condition information recited in independent claim 1 and the CW of *Wasilewski* are different. The condition information being updated in accordance with the usage of the main data aims to prevent the backup-restore attack. Specifically, the condition information is information that is updated in accordance with the usage of the main data and that is targeted to be backed up when the backup-restore attack occurs.

Furthermore, *Wasilewski* does not describe the type 1 key as recited in independent claim 1. Specifically, the Examiner refers to Col. 8, lines 48-60 of *Wasilewski* as describing "updating the type 1 key in accordance with the usage of the main data." From this reference, it appears that the Examiner equates the type 1 key recited in independent claim 1 with the CW of *Wasilewski*. However, the type 1 key and the condition information are different.

Moreover, the type 1 key is used by the second encrypting means to encrypt the type 2 key. Therefore, even if assuming the type 1 key is equivalent to the public key or private key used in the public-key encryption algorithm that is used to encrypt the MSK of *Wasilewski*, this assumption turns out to be incorrect because the type 1 key is updated by the second updating means in accordance with the usage of the main data, while the public key or private key in the set top unit (STU) is not updated in accordance with the usage of the main data in *Wasilewski*.

Accordingly, *Wasilewski* does not disclose a data usage controlling apparatus that decrypts the encrypted condition information using the type 2 key and includes second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key. For at least the reasons discussed above, Applicant submits that independent claim 1 is patentably distinct over *Wasilewski* and the rejection under 35 U.S.C. § 102(b) should be withdrawn.

Independent Claims 2, 9 and 10

Independent claims 2, 9 and 10 include similar features as recited in independent claim 1. For example, claim 2 is similar to claim 1, claim 9 is a data usage controlling method that corresponds to claim 1, and claim 10 is a computer-readable recording medium storing a program that corresponds to claim 1. Therefore, for at least this reason and the reasons discussed above for independent claim 1, Applicant submits that claims 2, 9 and 10 are patentably distinct over *Wasilewski* and the rejection under 35 U.S.C. § 102(b) should be withdrawn.

Dependent Claims 3-8

Claims 3-8 depend from independent claim 2, adding structural features that more particularly define the invention and further distinguish over the cited references and the prior art of record. For these reasons, and for the reasons set forth above for independent claim 2, the rejection of these dependent claims under 35 U.S.C. §§ 102(b) and 103(a) are improper and should be withdrawn.

Conclusion

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 27, 2005.

By: Lori Lapidario

Signature

Dated: July 27, 2005

Very truly yours,

SNELL & WILMER L.L.P.

Ketan S. Vakil
Registration No. 43,215
600 Anton Boulevard, Suite 1400
Costa Mesa, CA 92626-7689
Telephone: (714) 427-7000